RECEIVED
JUL 16 1993

Lawrence Livermore National Laboratory
Safeguards and Security Quarterly Progress Report
to the U.S. Department of Energy

OSTI

Quarter Ending March 31, 1993

Wayne D. Ruhter
R. Scott Strait
Doug L. Mansur
Greg Davis

April 1993

Lawrence
Livermore
National
Laboratory

This is an informal report intended primarily for internal or limited external distribution. The opinions and conclusions stated are those of the author and may or may not be those of the Laboratory.

Work performed under the auspices of the U.S. Department of Energy by the Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.

DISCLAIMER

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.

**This report has been reproduced
directly from the best available copy.**

**Available to DOE and DOE contractors from the
Office of Scientific and Technical Information
P.O. Box 62, Oak Ridge, TN 37831
Prices available from (615) 576-8401, FTS 626-8401**

**Available to the public from the
National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Rd.,
Springfield, VA 22161**

Table of Contents

Preface	LLNL-iv
Safeguards Technology Program	STP-1
Introduction.....	STP-1
Summary of Major Accomplishments.....	STP-1
Task Description and Quarterly Progress.....	STP-3
I. NDA MC&A Measurement Technology R&D	STP-3
• Intelligent Actinide Analysis System.....	STP-3
II. Emission and Transmission Computed Tomography.....	STP-4
• Detection Limits for Emission and Transmission Computed Tomography.....	STP-4
III. Support to DOE Facilities in Implementation, Testing and Evaluation of LLNL Developed NDA Techniques.....	STP-5
IV. Monte Carlo Simulation of Plutonium Gamma- Ray Spectra	STP-7
Appendix A: A Summary of all Milestones and Deliverables for the Quarter.....	STP-8
Appendix B: A List of all Publications Produced During This Quarter.....	STP-9
Safeguards Systems Studies	SSS-1
Introduction.....	SSS-1
Summary of Major Accomplishments.....	SSS-1
Task Description and Quarterly Progress.....	SSS-2
I. Safeguards Systems Studies No. LLNL 91019-93.....	SSS-2

II. Analysis of S&S requirements of Treaties that Impact DOE Mission.....	SSS-3
III. VA Fundamentals and ASSESS Courses.....	SSS-3
Appendix A: A Summary of all Milestones and Deliverables for the Quarter.....	SSS-4
Appendix B: A List of all Publications Produced During This Quarter.....	SSS-5
Computer Security - Distributed Systems	CSS-1
Introduction.....	CSS-1
Summary of Major Accomplishments.....	CSS-1
Task Description and Quarterly Progress.....	CSS-5
I. Distributed Intrusion Detection System and Network Security Monitor.....	CSS-5
II. OPSEC Detection of Classified Information on Unclassified Computer Systems	CSS-6
III. Distributed Audit Standards and Security Guidelines Development	CSS-6
IV. Security Profile Inspector for Unix and VMS.....	CSS-7
V. Computer Incident Advisory Capability (CIAC).....	CSS-9
VI. Computer Security R&D-CSPM.....	CSS-10
VII. Computer Viruses: Prevention, Detection and Mitigation.....	CSS-11
Appendix A: A Summary of all Milestones and Deliverables for the Quarter.....	CSS-12
Appendix B: A List of all Publications Produced During This Quarter.....	CSS-14

DOE Automated Physical Security.....	DAPS-1
Introduction.....	DAPS-1
Summary of Major Accomplishments.....	DAPS-1
Task Description and Quarterly Progress.....	DAPS-2
Appendix A: A Summary of all Milestones and Deliverables for the Quarter.....	DAPS-4
Appendix B: A List of all Publications Produced During This Quarter.....	DAPS-4

Preface

The Lawrence Livermore National Laboratory (LLNL) carries out safeguards and security activities for the Department of Energy (DOE), Office of Safeguards and Security (OSS), as well as other organizations, both within and outside the DOE. This document summarizes the activities conducted for the OSS during the second quarter of Fiscal Year 1993 (January through March, 1993).

The nature and scope of the activities carried out for OSS at LLNL require a broad base of technical expertise. To assure projects are staffed and executed effectively, projects are conducted by the organization at LLNL best able to supply the needed technical expertise. These projects are developed and managed by senior program managers. Institutional oversight and coordination is provided through the LLNL Deputy Director's office.

At present, the Laboratory is supporting OSS in four areas:

- Safeguards Technology
- Safeguard System Studies
- Computer Security
- DOE Automated Physical Security

The remainder of this report describes the activities in each of these four areas. The information provided includes an introduction which briefly describes the activity, summary of major accomplishments, task descriptions with quarterly progress, summaries of milestones and deliverables and publications published this quarter.

The LLNL welcomes the opportunity to apply its expertise in these technical areas. Although the aggregate of activities for OSS is modest, LLNL strives to provide quality responses to OSS needs and stands ready to assist OSS on these and other technical areas.

If OSS management or staff have questions about this report or LLNL's capability to assist in satisfying an OSS need, contact L. Lynn Cleland, 510/422-4951, or one of the program managers for the four technical areas.

Safeguards Technology Program

Wayne D. Ruhter, Program Manager
Nuclear Chemistry Division

INTRODUCTION

The Safeguards Technology Program (STP) is a program in LLNL's Nuclear Chemistry Division that develops advanced, nondestructive-analysis (NDA) technology for measurement of special nuclear materials. Our work focuses on R&D relating to x- and gamma-ray spectrometry techniques and to the development of computer codes for interpreting the spectral data obtained by these techniques.

SUMMARY OF MAJOR ACCOMPLISHMENTS

I. NDA MC&A Measurement Technology R&D

Intelligent Actinide Analysis System (IAAS)

- During the last quarter the IAAS was reassembled in the LLNL Plutonium Facility.
- Memory and disk upgrades to the Sun IPX workstation were installed.
- A software change and configuration management system has been implemented for the IAAS.
- A failed hard disk has been replaced and the disk system reinstalled.

II. Emission/Transmission Computed Tomography

- We have obtained a copy of the SYNTH code (a computer code used to generate synthetic gamma-ray spectra) and calibrated SYNTH using a measured ^{239}Pu spectra.
- The calibrated SYNTH code was used to calculate minimum detection limits for several transuranic nuclides.
- Preparations have been completed to perform a computed gamma-ray tomography measurement on a plutonium molten salt extraction button.

III. Support to DOE Facilities in Implementation, Testing and Evaluation of LLNL Developed NDA Techniques

- We modified the MGA code to account for interferences from weak gamma-rays from the decay of ^{234}Th in samples containing large quantities of ^{238}U .
- A reference version of the MGA code was created to act as the benchmark for future revisions. The reference version will be stored in a source code control system (SCCS) so that any code changes can be audited.
- We have tested the new solution analysis option in the MGA code against the old plutonium analysis code PUAN.
- An initial prototype of a MS Windows version of the MGA code was completed and is undergoing continuing refinement.
- A meeting was held at LLNL to discuss modifications to an instrument for measuring highly enriched ^{238}Pu at the Westinghouse Savannah River Company.

IV. Monte Carlo Simulation of Gamma-Ray Spectra

- We have improved the MCNP post-processing code that combines the Lorentzian distribution of the x-rays with the Gaussian distribution and tailing terms. (MCNP is a Monte Carlo Neutron Photon transport code.)
- We have completed a code for doing the Fourier transformation of the Augmented-Plane-Wave functions. This code allowed us to calculate the electron momentum distributions in various solids.
- The new super-scaler SPARC 10 processor was benchmarked with the MCNP codes. The new processor runs 2.7 times faster than the SPARC 2 processor.

TASK DESCRIPTIONS AND QUARTERLY PROGRESS

Accomplishments achieved during the second quarter of FY93 by STP are described below:

I. NDA MC&A Measurement Technology R&D

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060102	\$310K	\$213K

The overall objective for this task is to research and develop state-of-the-art nondestructive analysis (NDA) instruments, methods, and techniques that address top priority material control and accountability (MC&A) problems and will result in improved MC&A of SNM at DOE facilities. Activities include assistance to the field in resolving major and significant problems associated with holdup, heterogeneous materials, lump corrections, waste measurements, and shipper-receiver measurements.

Intelligent Actinide Analysis System

Zachary M. Koenig, William M. Buckley, Wayne D. Ruhter, and Austin L. Prindle

The intelligent actinide analysis system (IAAS) is a gamma-ray spectrometry system utilizing a distributed computer network that is intended to advance nondestructive actinide analysis systems for nuclear safeguards in performance, automation, ease of use, adaptability, systems integration, and extensibility to robotics. A major goal for these systems is a modular hardware and software design that will use commercially available components whenever practical to reduce development and maintenance costs. This will also allow easy modification for specific user requirements or technological extensions to the base instrument design. Another goal is to improve performance by assisting measurement technicians in setup and operation of the system for assurance of spectral data quality and results. The first system will be delivered to Materials Management at LLNL. Materials Management is supporting the hardware, documentation, and training costs.

During the last quarter the IAAS was reassembled in the LLNL Plutonium Facility. When the system was powered up one of the hard disks failed. This disk unit has been replaced and final testing of the IAAS is proceeding. Memory and disk upgrades to the Sun IPX workstation were installed. Software updates resulting from continued testing were also installed. A software change and configuration management system has been implemented for the IAAS.

II. Emission/Transmission Computed Tomography

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060102	\$150K	\$99K

This technology combines the advantages offered by two well-developed, nondestructive assay techniques: gamma-ray spectrometry and computed tomography (CT). Coupled together these two techniques may be used to nondestructively and quantitatively measure uranium and plutonium in samples where the U and/or Pu are heterogeneously distributed, distributed in lumps of varying size, or the sample matrix varies in density and composition. This technology potentially offers significant improvements over current segmented gamma-scanning (SGS) techniques.

Gamma-ray spectrometry passively and nondestructively measures the gamma-ray emissions from a sample. From the measured gamma-ray spectrum one can identify the radioactivities detected and determine their abundances, if appropriate corrections for sample self-attenuation are made. Transmission or active CT is a nondestructive technique, already widely used in medical and industrial applications, that uses an external-radiation beam to map photon attenuation within a sample. This attenuation data can be used to correct the emission data for sample self absorption. The result is an accurate, quantitative assay of all detectable radioactivities within a sample regardless of its form or composition.

Additional funding was received from the Office of Technology Development for the development of this technology and its application to waste drums. With this funding we have started with LLNL's Engineering Sciences Division the design of a prototype, single-detector, passive and active computerized tomography system called IMPACT (Isotope Measurements by Passive and Active Computerized Tomography).

Detection Limits for Emission and Transmission Computed Tomography

Tzu-Fang Wang, and David C. Camp

We have obtained a copy of the SYNTH code from Battelle Memorial Institute. This code uses algorithms with parameters to generate synthetic spectra from a point source geometry. We have used experimentally measured gamma-ray spectra of ^{239}Pu to calibrate the SYNTH code. SYNTH can then be used to reproduce measured gamma-ray spectra of other TRU nuclides inside various attenuation matrices. Using this calibration minimum detection limits (MDL) were calculated for ^{241}Am , ^{244}Cm , ^{239}Pu and $^{233,235}\text{U}$. Using these calculations we can predict MDL's for other TRU nuclides.

Several radiographs, of an inhomogeneous, weapons grade, plutonium, molten salt extraction button (MSE), have been made. The radiographs show regions of varying attenuation. A gamma-ray tomography apparatus has been moved from the LLNL site 300 area to the LLNL Heavy Element Facility to perform computed gamma-ray tomography on the MSE button. The radiograph shows the inhomogeneous material in two dimensions. We expect the computed tomography scan to map out the inhomogeneous material in three dimensions.

III. Support to DOE Facilities in Implementation, Testing and Evaluation of LLNL Developed NDA Techniques

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060302	\$103K	\$55K

The primary objective of this task is to assist DOE sites in implementation of LLNL developed NDA technology; in particular, assist Westinghouse Savannah River Company facilities; LLNL's Materials Management; and LANL's TA-55 facility. A brief description of activities under this task are given below.

In the last quarter we continued to support the LLNL plutonium reduction project. An additional 193 samples have been processed through the MGA isotopic analysis code.

In the process of analyzing the many types of plutonium samples, we encountered a series of samples containing very large quantities of ^{238}U relative to plutonium. To properly analyze these samples modifications to the MGA code were necessary to handle interfering gamma lines from the decay of ^{234}Th (a daughter activity from the ^{238}U decay series). A doublet (92.38 keV and 92.8 keV) from the ^{234}Th decay occurs in the spectrum from samples containing large amounts of ^{238}U . The position of these peaks is too close to where MGA selects its start position for fitting the 94 keV region, resulting in the starting position being placed on the high energy side of the doublet. MGA assumes that the start region is primarily background, so the fit results in a large negative residual between the start position of the region and the low energy side of the first peak in the grouping (94.6 keV). The start position was moved 0.5 keV higher in energy to correct the problem.

We also discovered an interference peak from the decay of ^{235}U in a sample containing large quantities of highly enriched uranium. We were able to use the GRPANL code to properly account for this interference at 345.9keV and use the low energy spectrum for the plutonium isotopic analysis. The MGA code will be modified to deal with this problem.

Since we now have the MGA code running on 3 computer systems, the decision was made to generate a "reference" version of MGA that would be the benchmark for future versions. The reference version will be the same for both DOS and UNIX systems. The VMS version will no longer be supported. This and all future reference versions of MGA will be stored in a source code control system (SCCS) so that any code changes can be audited. The PC reference version is almost complete and the current UNIX version will be aligned to the PC reference. Identification of the reference version will be with both internal SCCS id lines as well as a completely different sequence of version id lines that the code puts into it's output file.

We have tested the new solution analysis option in the MGA code against the old plutonium analysis code PUAN. The same spectra were run through both codes and compared. The two codes agree to within $\pm 0.3\%$.

An initial prototype of a MS Windows version of the MGA code was completed in January and is undergoing continuing refinement. A production prototype will be ready for demonstration at the INMM meeting in July. This version includes a graphical user interface with context sensitive help, a spectral viewing capability, and graphical viewing of the fitting results.

A meeting was held at LLNL on February 25, 1993 to discuss an upgrade to an instrument, at WSRC, for measuring isotopic abundances in highly enriched ^{238}Pu . The meeting was attended by Ken MacMurdo, Roy Clark and Rene Jacobson from WSRC and Wayne Ruhter, Austin Prindle, and William Buckley from LLNL. Modifications to the instrument are necessary to measure samples in different sample types of ^{238}Pu being shipped to WSRC from E. G. & G Mound Laboratory and the former USSR. WSRC has agreed to supply LLNL enough additional information so LLNL can put together a proposal to perform this upgrade.

William Buckley attended a class on measurement control for materials accounting, given at Los Alamos National Laboratory.

IV. Monte Carlo Calculations of Gamma-Ray Spectra

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060102	\$165K	\$67K

Monte Carlo Simulation of Plutonium Gamma-Ray Spectra

Zachary M. Koenig, Joseph B. Carlson, and Tzu-Fang Wang

The simulation of gamma-ray spectra for a known radioactive source, sample matrix, and geometry can be an important tool in designing and understanding non-destructive analysis (NDA) instruments such as Pu gamma-ray isotopic analysis systems. There are also a number of significant and major MC&A problems associated with heterogeneous materials, lump corrections, holdup, waste, and shipper-receiver measurements that can be addressed with this calculational tool. The gamma-ray spectra from each of these problems can be simulated with a Monte Carlo method by mocking up various geometries and transporting the gamma-rays of a known source through the material to a detector. Monte Carlo calculations may be used to calculate plutonium "standard" gamma-ray spectra that may be used to determine such characteristics as systematic biases in spectral data-analysis codes. With so many possible variations of the problems described above, the simulation of gamma-ray spectra from them is more efficient and cost effective than the development and measurement of various reference materials.

We have improved the MCNP post-processing code that combines the Lorentzian distributions of the x-rays with the Gaussian distribution and tailing terms. We now convolute the Lorentzian and Gaussian distributions and the tailing terms using continuous functions. The functions used to accomplish the spreading of the MCNP output are a complex error function, sine and cosine integral functions, and some fundamental functions. We have also completed a code for doing the Fourier transformation of the Augmented-Plane-Wave functions, thus obtaining the electron momentum distributions in various solids.

We have benchmarked the new super-scaler SPARC 10 processor with the MCNP codes. The new processor runs 2.7 times faster than the SPARC 2 processor.

APPENDIX A: A SUMMARY OF ALL MILESTONES AND DELIVERABLES FOR THE QUARTER

I. NDA MC&A Measurement Technology R&D

B&R No. GD060102

The Intelligent Actinide Analysis System was reassembled in the LLNL plutonium facility for final testing.

II. Emission/Transmission Computed Tomography

B&R No. GD060102

Minimum detection limits for several transuranic nuclides were calculated using a calibrated version of the SYNTH code.

Preparations have been completed to perform computed gamma-ray tomography on a molten salt extraction button.

III. Support to DOE Facilities in Implementation, Testing and Evaluation of LLNL Developed NDA Techniques

B&R No. GD060302

An initial prototype of a MS Windows version of the MGA code was completed.

The MGA code solution analysis option was tested against the older solution analysis code PUAN.

A reference version of MGA to be used as a benchmark for future revisions was created and stored in a source code control system.

IV. Monte Carlo Calculations of Gamma-Ray Spectra

B&R No. GD060102

We have improved the MCNP post-processing code that combines the Lorentzian distributions of the x-rays with the Gaussian distribution and tailing terms.

We have benchmarked the new super-scaler SPARC 10 processor with the MCNP codes.

APPENDIX B: A LIST OF ALL PUBLICATIONS PRODUCED DURING THIS QUARTER

There were no publications this quarter.

Safeguards Systems Studies

**R. Scott Strait, Deputy Associate Program Leader
Fission Energy and Systems Safety Program**

INTRODUCTION

The purpose of the program is to develop systematic approaches and analytic tools for evaluating and enhancing the effectiveness of safeguards and security systems. We develop methodologies and tools for evaluating material control and accountability systems, measures protecting against insider threats, and measures that may contribute to the deterrence of threats. We transfer the technology developed through workshops and field consultations, and we evaluate available tools to determine their applicability to DOE safeguards and security interests. We also provide technical support to OSS on program planning, assessment and integration, and implications of arms control treaties.

SUMMARY OF MAJOR ACCOMPLISHMENTS

- Completed testing and revisions to ASSESS software.
- Updated ASSESS User's Manual to reflect changes in the software made. The completed User's Manual will be published and made available for the May ASSESS Course.
- Enhanced algorithm for software for evaluating violent insiders using force against barriers.
- Supported the Central Training Academy in the teaching of one VA Fundamentals course.
- Provided technical support to OSS on developing approaches to planning for possible CWC on-site inspections.
- Reviewed DOE S&S Orders for consistency with requirements for hosting CWC inspections. Identified areas of conflict and possible revisions.

TASK DESCRIPTIONS AND QUARTERLY PROGRESS

I. Safeguards Systems Studies LLNL 91019-93

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD 06-02-05	\$230K	\$155K

This task develops systematic approaches and analytic tools for evaluating and enhancing the effectiveness of safeguards and security systems. We develop methodologies and tools for evaluating material control and accountability systems, measures protecting against insider threats, and measures that may contribute to deterrence of threats. We also transfer the technology developed through workshops and consultations, as needed. We provide field assistance in the application of evaluation methods, and tools. We evaluate available tools to determine their applicability to DOE safeguards and security interests.

This quarter, we completed the software development for all features slated for this fiscal year. This software will be used during ASSESS training in May, and any software changes during the rest of the fiscal year will be to correct bugs or to provide minimal user interface enhancements, such as word changes in dialog boxes or help screens. We also updated the ASSESS User's Manual to reflect changes in the software made this fiscal year. Most of these changes were minimal in nature, updating pictures of the screen displays, etc. One section that required significantly more effort was the Hand-off Collusion module section. For this section, we needed to create example files suitable for inclusion in the manual, as well as update the text and the displays. This quarter we also enhanced the software and algorithm for the prototype software for evaluating insiders using violence against barriers, and we continued to refine the MC&A database.

This quarter we were requested by OSS to review the ASSESS code and databases for the presence of UCNI. Although ASSESS had once before been reviewed for UCNI, the review took place prior to the issuance of specific Safeguards and Security UCNI guidance from DOE-HQ. Two LLNL personnel were trained as UCNI Reviewing Officials and reviewed the code, databases, and documentation. It was determined that the ASSESS databases contain UCNI. However, no UCNI is contained in the User's Manual, algorithms, or user interface. As a related issue, per OSS request, we gathered information for including ASSESS in DOE's Energy Science and Technology Software Center (ESTSC). We have gathered information, included required legal notices and disclaimers in the code and User's Manual, and are preparing a submittal to ESTSC. A memo to OSS (joint from LLNL and SNL) summarizing these efforts is being prepared.

II. Analysis of Safeguards and Security Requirements of Treaties that Impact DOE Mission

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD 05-08-03	\$207K	\$56K

This task provides OSS with comprehensive technical reviews of the safeguards and security implications of pending arms control treaties. Under this task, we analyze impact on DOE sensitive facilities and related inspection readiness planning requirements. We also evaluate alternative approaches to readiness to determine most efficient methods to achieve treaty compliance and protect DOE vital assets.

This quarter we provided technical support to OSS on developing an approach to planning for possible CWC on-site inspections and for possible bilateral (U.S. and Russia) chemical weapons treaty inspections. We reviewed all DOE S&S Orders for consistency with requirements for hosting CWC inspections. We identified areas of conflict and possible revisions. We noted that most DOE S&S orders appeared to be amenable to challenge inspections without revision. There are a few orders, however, that may require modification or exceptions to accommodate such inspections. We also noted that there are areas in which additional awareness, guidance and/or training may be appropriate.

III. VA Fundamentals and ASSESS Courses

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD 05-06-02	\$90K	\$51K

This task supports the DOE CTA in presenting safeguards courses in areas of LLNL expertise. In this quarter, we supported CTA in presenting one VA Fundamentals course. We have one VA Fundamentals course and one ASSESS course remaining this fiscal year.

APPENDIX A: SUMMARY OF MILESTONES AND DELIVERABLES:

I. Safeguards Systems Studies LLNL 91019-93

B&R No. GD 06-02-05

The VA Newsletter, published jointly with Sandia, was scheduled for February. We requested and received from OSS a delay in this newsletter to accommodate an UCNI review of ASSESS. The newsletter will be published and distributed to field users next quarter.

The ASSESS Documentation reflecting new software features was completed. It is being prepared for distribution at the upcoming ASSESS Course.

II. Analysis of Safeguards and Security Requirements of Treaties that Impact DOE Mission

B&R No. GD 05-08-03

Completed review of DOE S&S orders for applicability of those orders to the hosting of CWC inspections. Prepared reports for DOE.

III. VA Fundamentals and ASSESS Courses

B&R No. GD 05-06-02

VA Fundamentals Course presentation at the Central Training Academy, February 1-5, 1993.

APPENDIX B. A LIST OF ALL PUBLICATIONS PRODUCED DURING THIS
QUARTER

There were no publications this quarter.

Computer Security — Distributed Systems

Doug L. Mansur, Program/Division Leader
Computer Security Technology Center

INTRODUCTION

The overall goal of the Computer Security Technology Center (CSTC) is to develop innovative solutions to the computer security problems of the Department of Energy and other US Government agencies. Activities are currently underway in such diverse areas as host and network intrusion detection, computer virus and malicious code research, system security configuration maintenance, and other special projects. The program also supports the DOE community through the Computer Incident Advisory Capability (CIAC), which responds to computer security incidents, and performs other critical activities such as research on system and network vulnerabilities, available protection technologies, and threat information.

SUMMARY OF MAJOR ACCOMPLISHMENTS

I. Distributed Intrusion Detection System and Network Security Monitor

Expansion of the Distributed Intrusion Detection System (DIDS) continues toward the goal of making the system capable of monitoring VMS host systems. Documentation of the initial VMS host monitor implementation is near completion. Further work on DIDS has been suspended until additional funding becomes available--the primary focus will now be on improving the usability of the Network Security Monitor (NSM).

A system analysis of the current NSM has begun using the latest reverse-engineering tools, with a goal towards carefully documenting the current design and implementation. Current users are being asked to recommend improvements to the usability and functionality of the product. Research is being done on expanding the NSM so that it is capable of handling multiple connected LAN segments. A future version will allow a single security officer to observe activities on multiple LANs.

II. OPSEC Detection of Classified Information on Unclassified Computer Systems¹

The initial prototype has been undergoing testing against real data sets to test both the speed and effectiveness of the software in real-world situations. Successful detection of classified information under controlled conditions was accomplished. Discussions continue with OSS and other organizations on the use of this software to monitor high-to-low file transfers, perform pre-publication backup reviews of documents, and detect potentially misplaced information. This task was funded initially by OSS in FY92 and continues under internal and work-for-others funding.

III. Distributed Audit Standards and Computer Security Guidelines Development

Copies continue to be sent to DOE sites requesting the first version of the VMS Security Guideline. SPARTA has begun discussions with LLNL on the update to this document so that the document may include information on the latest security changes to VMS Versions 5.X and 6.0.

The next phase of research to be performed on the Distributed Audit Standards (DAS) will analyze in greater detail the specific audit information that must be collected and transmitted across the network for successful monitoring. Further work is in the planning stages on making the initial design of DAS more robust and complete. SPARTA is being encouraged to expand its interactions with the national and international standards organizations in this area.

IV. Security Profile Inspector for UNIX/VMS

The Security Profile Inspector (SPI) development team continues to make rapid progress in the creation of SPI version 3.0. This new product will accommodate both UNIX and VMS systems in a single package, utilizing many of the same modules and a common user interface. A SPI Query Language System has been developed to permit rapid future expansion of the set of tests performed by SPI--particularly during a major incident. The Query Language System interfaces with the data extraction subsystem to pull out of a given computer the specific security information required for a given test.

¹ This task was originally funded by DOE/SA in FY92 and is currently funded from other sources. We include it for information only.

SPI has been recently ported to Plexus and Oncore Multimax systems running their own versions of UNIX. At present the SPI software runs on a wide variety of UNIX-type workstations, PC-style computers, and mainframes.

The Forum for Incident Response Security Teams (FIRST) has requested that LLNL work with Dr. Gene Spafford of Purdue University to form an industry standard for a mechanism to check the integrity of system software. A universal standard is needed to permit widespread development and sharing of file integrity cryptochecksums.

V. Computer Incident Advisory Capability (CIAC)

The Computer Incident Advisory Capability (CIAC) continued to assist DOE sites with incidents, as well as provide research into new security vulnerabilities requiring immediate remedy. New virus outbreaks continue to plague the DOE community and responses are being coordinated with other virus experts to ensure the availability of the latest detection tools.

CIAC presented four incident handling training workshops during this quarter and attempted to target the discussions at either management or technical audiences as appropriate.

Several CIAC Advisory Notices and Information Bulletins were issued during the past quarter, including those addressing problems with DEC/VMS, Cray/UNICOS and Sun/OS systems, among others. In addition, many DOE sites received information via the Felicia and Irbis repositories.

A preliminary research effort has begun to investigate the feasibility of a tool to assist sites which may be experiencing a given type of attack to uncover which systems may be vulnerable. Such a tool would be designed to scan all systems on a given local network to check whether they were susceptible to external attack of a known type.

VI. Computer Security R&D-CSPM

The primary individual on this task (Chuck Cole) has received a promotion to Deputy Associate Director for Compliance in the Computations Organizations. Continued work on this task will be carried out by Harry Bruestle, the new deputy program leader for CSTC. Work will continue on the overall classified computer security program planning document, as well as specific investigation into requirements concerning security testing and evaluation for the OSS program.

VII. Computer Viruses: Prevention, Detection, and Mitigation

The University of California Davis continues to work with the CSTC on research in malicious code detection and analysis. Improvements are continuing in the ability to use both static and dynamic analysis techniques in a combined effort to deal with the latest stealth and polymorphic viruses. Current detection technology is unable to handle these new threats. UC Davis continues to collect information on suspicious behavior characteristics of malicious code so that signatures may be developed that are robust and general enough to span multiple malicious code types.

TASK DESCRIPTION AND QUARTERLY PROGRESS

I. Distributed Intrusion Detection System and Network Security Monitor

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060103	\$53K	\$53K

Work continued on the development of the Distributed Intrusion Detection System (DIDS) VMS Host Manager software. Configuration programs that build the databases for the VMS DIDS Host Monitor were built and tested. The implemented databases were based on the UNIX Host Monitor databases. External documentation for the DIDS software was drafted.

Further work on DIDS has been suspended until additional funding becomes available from the DoD. Concentration on improvements to the NSM is the current primary focus.

Bob Palasek has begun a systems analysis, interviewing users about how the Network Security Monitor (NSM) is presently being used and has also begun using a software reverse-engineering tool available at LLNL to document NSM's internal structure. The goal is to make the product easier to use, moving it closer to a plug and play capability for those customers with a large computing-base, but not possessing a cadre of graduate level network managers.

Bob will also explore the feasibility of incorporating additional network protocols into the NSM package. He is also looking into "productizing" NSM, identifying the issues associated with a wider distribution.

We are working on a method for dealing with multiple interconnected LAN segments. Presently the NSM runs as a separate monitor on each LAN and an improvement permitting LAN-to-LAN communication and coordination is highly desirable. Other areas being improved include the heuristics used to sort user sessions based on their likelihood of involvement in an attack, and methods to model attack signatures.

II. OPSEC Detection of Classified Information on Unclassified Computer Systems

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060103	-0 ²	N/A

The goal of this project is to develop and demonstrate the capability to perform automated searches of unclassified systems to detect the possible presence of classified or otherwise sensitive information. The analysis process is driven by a keyword-relationship table specifying word linkages that represent sensitive phrases or concepts. The calibration of the prototype software continues at LLNL on known classified information. A recent test on a text file of congressional testimony, known to be classified (and later sanitized for release), showed a relatively high correlation between statements that are sensitive and the statements flagged by the analysis tool. This has proven to be an excellent test of the initial prototype.

Discussions and planning continue toward using the present tool as a filter in a file transfer system. The goal is to replace the so-called "sneaker net" method of the file transfer (which is unacceptable) with a carefully designed, authorized, and fully monitored direct means for file transfer.

III. Distributed Audit Standards and Computer Security Guidelines Development

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060103	\$95K	\$95K
GD060303	\$31K	\$31K

Requests are still being received for the latest version of the VMS Guideline. SPARTA continued to revise the guideline to encompass security considerations for VMS version 5.X and 6.0. Significant improvements to the DEC VMS operating system have been made since the last VMS Guideline update. Users will be able to more easily understand and use these new security features once the new guideline is completed.

² This task was originally funded by DOE/SA in FY92 and is currently funded from other sources. We include it for information only.

Discussions with SPARTA, Inc. have occurred concerning the next phase of the research into distributed audit standards. SPARTA is preparing to present at the '93 DOE Computer Security Government Conference a paper titled "A Distributed Audit System (DAS) Using Network Management Protocols." This will highlight for the DOE infosec community the work done to date, and near-term plans to strengthen and improve the current design. A major goal is also to work with the national and international standards organizations to get improved auditing capabilities into commercial systems that would then be available for DOE use.

Expansion of the management information base (MIB) is necessary in the next research phase to encompass more of the types of specific audit information which will be necessary for successful real-time detection of unauthorized activity. We anticipate that this schema will also aid in the inter-site sharing of audit information, so that experienced individuals can act as advisors to other sites by allowing them to rapidly see complete sets of remote audit information.

IV. Security Profile Inspector for UNIX/VMS

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060103	\$189K	\$160K
GD060103	\$189K	\$160K

The Security Profile Inspector (SPI) software packages, for both UNIX and VMS systems, provide tools to security officers for maintaining DOE's secure computing environments.

These projects are jointly funded by DOE/SA and the US Air Force, with new funding expected from the Defense Information Systems Agency. The present versions of both products continue to be distributed on a regular basis, and as individual requests arrive. SPI/UNIX 2.1 is available electronically via anonymous FTP of the [irbis.llnl.gov](ftp://irbis.llnl.gov) file server and SPI/VMS 1.2 is available via FTP of [ADDVAX.LLNL.GOV](ftp://ADDVAX.LLNL.GOV). Both packages can be requested on tape, although transfer of this function to OSTI and/or a commercial entity is now being investigated.

Tony Bartoletti is coordinating the activities of Susan Taylor and Steve Cooper as work proceeds on SPI 3.0, a product suite designed to accommodate both UNIX and VMS security inspections in both single host and distributed operational modes.

Steve Cooper has specified the fundamental objects for the unified UNIX/VMS security model, with implementation of the supporting C-code library for the UNIX side nearing completion. The single inter-mediating C-call interface library will be used for both the UNIX and VMS operating systems to greatly reduce development costs. These calls will be used to extract security-related system data for analysis by the SPI inspection modules.

Susan Taylor has implemented the SPI Query Language System, which will act as a front-end for the data extraction library and perform the primary data analysis. Successful (stubbed) alpha testing has been conducted. The Query System accepts flexible scripts to direct varied and conditional security queries. Integration testing of the combined Data Extractor and Query System is expected to be conducted in April.

Tony has conducted successful integration tests of the SPI Change Detection Tool, Database Manager, and Report Generator, and has produced UNIX-style "man" pages for these utilities. He also worked with Susan Taylor to make enhancements to the Report Generator, accommodating the variability of output expected of the SPI Query Language System.

Tony has written to Dr. Gene Spafford of Purdue to form a working group aimed at developing standardized (multi-vendor) tables for file system integrity. The goal is to encourage vendors to maintain and make available tables which can be used to positively identify individual file objects, revisions, and patch-ids. The current lack of such information and standards is a major impediment to effective system integrity evaluation. The BIT Binary Inspector Tool depends upon such tables, which must be laboriously compiled and regularly revised.

Technical support has been provided to users from LLNL and BNL, as well as DISA, Air Force, and Navy sites. SPI/UNIX announcements, FTP instructions, manuals, UNIX security educational materials, and the SPI Usage Questionnaire were distributed to the 59 DOE CPPCs and CPPMs.

Tony provided technical support to Mark Barber on a SPI port to a Plexus (SysV) and an Oncore Multimax (SysV, R2.4, 2.4.u, NS32532). He worked with Herb Langenbach (BNL) to isolate a SPI problem which occurs on the HP-9000/375 series. In the course of this investigation, Tony discovered and fixed a problem in SPI gecos-field parsing, and subsequently placed a new SPI distribution (spi2.1E.tar) on irbis.

Tony wrote to Carl Dichter of Motorola Corporation regarding the current SPI/Unix features. Carl is writing an article on "affordable" computer security tools. He also wrote a reply to John Wack of NIST on the issue of SPI distribution. Tony also prepared a SPI LLNL distribution report for Lonnie Moore, LLNL Computer Security.

V. Computer Incident Advisory Capability (CIAC)

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060303	\$490K	\$393K

The Computer Incident Advisory Capability (CIAC) team members continued to assist users at DOE sites. Incidents, problems, and vulnerabilities such as network probes and intrusions, automated attacks, virus outbreaks and other events continue to plague the community.

CIAC presented four workshops during this quarter. These were held at DOE Headquarters in both the Germantown facility and at the Forrestal Building. Each location was offered both the Incident Handling for Managers class and the Technical Incident Handling class. The CIAC sponsors suggested that the Incident Handling for Managers class be restructured and shortened to appeal to a higher level audience. This is being done now. Preliminary suggestions include changing the name of the workshop to Incident Handling for Executives.

CIAC issued the following bulletins during this quarter:

- D-06 Failure to disable user accounts for VMS 5.3 to 5.5-2
- D-07 UNICOS running MLS, UNICOS environment variable (restricted dist.)
- D-08 Potential Vulnerability in VMS V5 and Derivative Op Systems
- D-09 OpenVMS VAX Security Patch #1084, Addendum to CIAC D-08
- D-10 November 17 Virus on MS DOS Computers
- D-11 Sun Security Patches and Software Updates

CIAC statistics of general interest for the quarter:

Contacts	402
Logons to Felicia	197
Logons to Irbis	505
Files Transferred	5030
E-Mail Messages	535

An E-Mail message was posted from the Commonwealth of Independent States (CIS, the former Soviet Union) to several US sites inquiring about a VMS security vulnerability. CIAC's excellent relationship with Digital Equipment Corporation security personnel allowed us to be first in the nation to release information and procedures to fix this vulnerability.

In an unrelated incident, Karyn Pichnarczyk investigated and researched an E-Mail message that originated in the CIS that asked for lists of user names from several locations on the Internet.

CIAC team members provided assistance to a DOE site that suffered a series of unauthorized accesses to an ftp server. These accesses involved the transfer of material of a highly sensitive nature, thus it was important that this incident be resolved quickly. We helped the system manager secure the ftp file system and erase the material.

Karyn Pichnarczyk spent a great deal of time working on the November 17 virus outbreak. This was a major incident in the DOE community. She was the primary contact for the DOE community on technical issues relating to this virus. Karyn's analysis and quick response helped the community avoid a much more widespread event.

Steve Weeber was alerted by a system administrator at a DOE site of suspicious activity on a machine. The machine had been penetrated by a network intruder apparently originating from Italy. Steve helped the system administrators at both the affected DOE site and the organization in Italy to secure their machines. Steve Weeber and Steve Mick provided information in an interview with Special Agent James Treacy of the foreign counter-intelligence unit of the FBI.

Steve Mick presented a CIAC Program Review at DOE Headquarters. This review went very well. The items and topics discussed included:

- Current CIAC project activities
- Schedule/timing of CIAC funding, especially at the start of the fiscal year, possible multi-year funding for CIAC
- CIAC's relationship and support of the ER community, notably ESnet
- Cost reduction measures and suggestions
- CIAC Workshop schedule, and
- Status of Privacy Enhanced Mail (PEM) in the federal community

VI. Computer Security R&D-CSPM

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060303	\$250K	\$68K

We began to direct our efforts toward developing an understanding of the testing and certification problem domain as it relates to the diverse computer systems/networks within the DOE community. In anticipation of our involvement with the development of a formalized testing and certification

strategy, we have begun to hold informal discussions with experts in the area, to research and collect open literature, and to collect requirements.

VII. Computer Viruses: Prevention, Detection, and Mitigation

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD060103	\$53K	\$53K

A contract has been placed with the University of California at Davis to begin the next research work in malicious code detection and analysis. UC Davis will continue to improve the static and dynamic analysis capabilities developed by them to pursue the latest problems with polymorphic (mutating) and "stealth" viruses.

Analysis of an encrypted virus will be done using the dynamic tool up to the point that the virus has decrypted itself. At this point static analysis will be activated to continue the analysis process.

UC Davis has been tasked to build a library of suspicious behavior. With this library it will be possible to analyze software for these specific symptoms and flag any occurrences for further detailed hand analysis. Of particular interest are malicious code signatures which are highly specific (low false positives), easy to observe, and difficult to intentionally mask.

Discovery of new viruses around the world at an ever-increasing rate, and the creation of viruses which are more and more difficult to detect, will require fundamentally new methods of detection in the future.

APPENDIX A: A SUMMARY OF ALL MILESTONES AND DELIVERABLES
FOR THE QUARTER

I. Distributed Intrusion Detection System and Network Security Monitor

B&R No. GD060103

A system analysis of the current NSM has begun.

II. OPSEC Detection of Classified Information on Unclassified Computer Systems³

B&R No. GD060103

The testing of real classified files has begun.

III. Distributed Audit Standards and Computer Security Guidelines Development

B&R No. GD060103 & GD060303

No milestones or deliverables are present for this quarter.

IV. Security Profile Inspector for UNIX/VMS

B&R No. GD060103

A SPI Query Language System has been developed to permit rapid future expansion of the set of tests performed by SPI--particularly during a major incident.

SPI has been recently ported to Plexus and Oncore Multimax systems running their own versions of UNIX.

³ This task was originally funded by DOE/SA in FY92 and is currently funded from other sources. We include it for information only.

V. Computer Incident Advisory Capability (CIAC)

B&R No. GD060303

A research effort has begun to investigate the feasibility of a tool to determine which systems at a site may be vulnerable to a given type of attack.

VI. Computer Security R&D-CSPM

B&R No. GD060303

No milestones or deliverables are present for this quarter.

VII. Computer Viruses: Prevention, Detection, and Mitigation

B&R No. GD060103

No milestones or deliverables are present for this quarter.

APPENDIX B: A LIST OF ALL PUBLICATIONS PRODUCED DURING THIS
QUARTER

None to report this quarter

DOE Automated Physical Security

Greg Davis, Program Manager

INTRODUCTION

The goal of the DOE Automated Physical Security task (DAPS) is to enhance the LLNL developed Argus Integrated Security system to meet DOE security needs and to transfer Argus to the private sector.

The objective is to identify interested companies, generate and provide technical information describing the Argus system, and enter negotiations with the intention of transferring the Argus technology. The transfer may take the form of CRADAs and/or licenses. The licenses may be exclusive for a limited period of time or in a limited market sector.

SUMMARY OF MAJOR ACCOMPLISHMENTS

- I. All field equipment has been installed in the badge offices and in the test building T1677 for the biometric test. Badge office biometric enrollment software was installed with Argus Release-12. Biometric enrollments have begun in preparation for starting the test. All software needed for the field test has been designed, written, and tested. Host software to support the field test was installed on 4/15/93 along with the Argus Release-14.
- II. CRADA discussions focused on a consortium of 3 companies. Martin Marietta Corporation (MMC), Digital Equipment Corporation (DEC), and Texas Instruments (TI) were given a letter of intent to negotiate a CRADA which was signed by the head of the LLNL Technology Transfer Department. Only MMC and DEC signed and returned the letter. Meetings were held to discuss technical aspects of the Argus system and to set the ground work for a Joint Statement of Work.

An Argus system overview presentation was developed and given to interested vendors. A series of photographs were taken showing all major elements of the Argus system.

- III. Greg Davis and J. Smart visited the laboratory at the Hanford facility where Smart Card and biometric capabilities are being developed. Rob Nelson demonstrated the 3-D HGU biometric integration with the Smart Card.

TASK DESCRIPTIONS AND QUARTERLY PROGRESS

I.

<u>B&R No.</u>	<u>Funding</u>	<u>Obligated</u>
GD 06 0201	\$325K	

Argus Enhancement

This effort is intended to demonstrate compliance with current DOE orders and enhance the Argus system to bring it in line with the latest DOE security orders. This should make it more appealing and immediately usable by potential commercial transferees. These activities include an Argus compliance evaluation, implementation of two-person rule in the Access control system, and evaluation of the fielding of the DOE selected 3-D hand geometry biometric reader in the Argus access control system. SA-10 will participate in the evaluation of Argus compliance.

The compliance matrix that we now have is being expanded to cover more DOE orders. Dave Fortney and Erv Behrin have identified a larger set of orders to be reviewed and they have started listing specific Argus related items in the orders.

The two-person rule work has been delayed to allow coordination with the work that we are doing for Pantex effort. We believe that this can yield two-person rule functionality which would be implemented on our production system rather than the planned simple demonstration on our development system.

We are ready to begin the testing of the biometric capabilities of the Argus system. All that remains is to field the new booth software. The booth software awaits installation following the Release-14 initial operational testing period. This is expected to take place the week of April 26. The test will include statistics on false rejection, trends in scoring the hand reads, and user acceptance of the system. Biometric enrollments at the badge office is now a routine procedure.

Technology Transfer

These activities include the generation of technical information describing the Argus system to potential transferees, briefing and touring interested parties, and negotiating and executing agreements for the formation of CRADA's and licenses. There will also be interaction with DOE to identify and address any security concerns arising from the transfer of Argus technology.

This has been the most active area of this task.

Meetings, briefings, and tours have been conducted with technical and business elements of the consortium.

Questions have arisen with regards to the policy of transferring DOE security technology. Discussions regarding the protections of DOE interests and the maintenance of security have been held at Livermore and at DOE Headquarters.

Guidelines for Argus technology transfer and CRADA formation are being developed and will be provided for review next quarter.

Smart Card Evaluation

LLNL will participate in the evaluation of a Smart Card system to transfer DOE clearance information. This will be done as an option to streamline the classified visit process.

Dave Palmer at Hanford was visited and the Smart Card efforts were reviewed. A special purpose system for access control was demonstrated. An individuals biometric information is written to the Smart Card and used to validate that the individual presenting the card is the same individual who was enrolled.

We have not yet sought or received guidance on the acquisition of a prototype Smart Card system that we may evaluate. This will become a high priority in the third quarter.

APPENDIX A. A SUMMARY OF ALL MILESTONES AND DELIVERABLES FOR THE QUARTER

DELIVERABLE STATUS TABLE

Original Deliverable	Description of Deliverable	Status
12/31/92	Provide DOE with a list of candidate vendors who we believe are interested in accepting the ARGUS technology.	Delivered 1/12/93
01/29/93	Demonstrate to DOE the ARGUS two-person rule capability.	Delayed
02/28/93	Demonstrate the operation of the 3-D hand geometry device at Building T1677 at LLNL.	Delivered 4/23/93
03/30/93	Provide to DOE technology transfer documentation and information.	Partial Delivery. More to come
09/30/93	Provide a report summarizing the technology transfer effort, the application of technologies and potential upgrades investigated, and recommendations on future enhancements to this system.	On schedule
09/30/93	Provide a final report on the evaluation of the biometric device at LLNL.	On schedule

APPENDIX B. A LIST OF ALL PUBLICATIONS PRODUCED DURING THIS QUARTER

None

END

**DATE
FILMED**

9/2/93